

REMARKS

This responds to the Office Action mailed September 7, 2004. Claims 1-14 remain pending, and have been amended herein. Claims 1, 7 and 11 are the independent claims.

Title

The title has been amended as suggested by the Examiner.

Information Disclosure Statement

The applicant's filed in Information Disclosure Statement (IDS) and form PTO-1449 on July 27, 2001. An initialed copy of the form PTO-1449 is respectfully requested.

Amended Claims

It is respectfully submitted that the amended claims define over the documents cited by the Examiner in the first Office Action, namely, U.S. Patent No. 6,069,955 to Coppersmith et al. (Coppersmith) and U.S. Patent No. 5,864,665 to Tran (Tran).

More particularly, claims 1 to 14 have been amended to replace the terms private and public data with the terms private and public *plain text*, respectively. There is a fundamental difference between the public and private data of the current invention and the public and private keys disclosed in *Coppersmith*. A cryptographic key is a mathematical value that is used in an encryption process to encrypt a message comprising plain text. The data used in the current invention refers to the message that is to be encrypted and not the key that is used in the encryption process. Hence the data of the current invention

can be equated with the "serial number" in *Coppersmith* (see col. 4, lines 1 to 5). Thus there is a fundamental difference between the technologies.

To clarify this difference, the terms public data and private data have been amended to public plain text and private plain text. The terms 'plain text' and 'key' are well known in the art, and the difference between them will be clear to the skilled person.

Furthermore, *Coppersmith* teaches a verification method using first and second private key and public key pairs (see figure 1 and col. 3, lines 1 to 59). A security code 102 is encrypted using a private key 103 and is printed onto a visible label 107 via a printer 105. A second serial number is encrypted by the private key 104 and is printed onto a hidden label 108 by printer 106 (see col. 3, lines 41 to 49). To perform the verification process the customer examines the visible label using the public key 109, and after purchase, examines the hidden label using the public key 110 (see col. 3, lines 49 to 59).

Thus the private keys are used entirely for the purposes of *generating* encrypted codes and the public keys are used entirely for the purposes of *verification*. This is confirmed at column 2 lines 58 to 67 of *Coppersmith*.

This is in contrast to the method of amended claim 1, wherein both the public plain text and the plurality of private plain text sets are used to generate encrypted security codes. In

the verification process, the public plain text and the plurality of private plain text sets held by the verifier are entered into the predetermined encryption algorithm to produce a *list of security codes*. Thus, even assuming for the sake of argument that the Examiner's view is taken, i.e., that the private and public keys of *Coppersmith* are equivalent to private and public plain text of the present development, the steps for generating encrypted security codes and verifying the authenticity of the goods are still different.

Furthermore, claim 1 requires both public and private plain text in both instances which makes it a secure process, whereas the methods of *Coppersmith* only relate to use of private keys for producing encrypted security codes and the use of public keys for the verification process.

Also, the feature of the "list of verification codes" recited in amended claim 1 is more than a convenient method of organizing the verification codes; it is indicative of the fundamental difference between the method of claim 1 and the method of *Coppersmith*. In *Coppersmith*, only one verification code is generated per verification action. In the verification process of claim 1, both the public plain text and the plurality of private plain text sets are entered into the encryption algorithm, which generates *all the verification codes* associated with the product. The comparison is then made with the list. *Coppersmith* does not disclose or fairly suggest generation of a list since only one code is decrypted by the public key during a

verification action, thus producing one decrypted number for comparison with the serial number printed on the label.

For the above reasons it is respectfully submitted that claim 1 defines over and is not rendered obvious by *Coppersmith*.

Claims 7 and 14 include a security code having been produced by means of a predetermined encryption algorithm from said public plain text and a plurality of private plain text sets. It is respectfully submitted that amended claims 7 and 14 are also patentable over the cited documents.

Nothing in *Tran* overcomes the deficiencies of *Coppersmith* with respect to the amended claims. The dependent claims are submitted to be allowable with their respective base claims.

Respectfully submitted,



Steven M. Haas (Reg. No. 37,841)
Fay, Sharpe, Fagan, Minnich & McKee, LLP
1100 Superior Ave - Seventh Floor
Cleveland, Ohio 44114
(216)861-5582